



ПРАКТИКА РЕАЛИЗАЦИИ МЕР ПО ЗАЩИТЕ ОБЪЕКТОВ КИИ

Зенков Александр

Руководитель инженерно-технического
департамента



Опыт применения СрЗИ при защите КИИ

Меры обеспечения безопасности значимого объекта	Продукт
I. Идентификация и аутентификация (ИАФ)	Dallas Lock, SecretNet, KICS For Networks, JMS, встроенные компоненты ОС или SCADA
II. Управление доступом (УПД)	ОРД, Dallas Lock, SecretNet, JMS, Аккорд, Соболев, VPN, встроенные компоненты ОС или SCADA
III. Ограничение программной среды (ОПС)	ОРД, KICS for Nodes, Kaspersky Security Center
IV. Защита машинных носителей информации (ЗНИ)	Dallas Lock, SecretNet, DLP, KICS for Nodes, KSC
V. Аудит безопасности (АУД)	ОРД, KICS for Nodes, KSC, staffcop, Стахановец, TimeInformer, FalconGaze SecureTower, SpectorSoft, RedCheck, MaxPatrol 8, MaxPatrol SIEM, ViPNet IDS, COA «Континент», АПК «Рубикон», RedCkeck, Сканер-BC
VI. Антивирусная защита (АВЗ)	ОРД, антивирусы, KICS for Nodes/KICS for Networks
VII. Предотвращение вторжений (компьютерных атак) (СОВ)	ОРД, ViPNet IDS, COA «Континент», UserGate, KICS for Nodes/KICS for Networks
VIII. Обеспечение целостности (ОЦЛ)	ОРД, KICS for Nodes, KICS for Networks, TimeInformer, FalconGaze SecureTower, SpectorSoft, встроенные компоненты ОС или SCADA
IX. Обеспечение доступности (ОДТ)	ОРД, КиберБекап



Опыт применения СрЗИ при защите КИИ

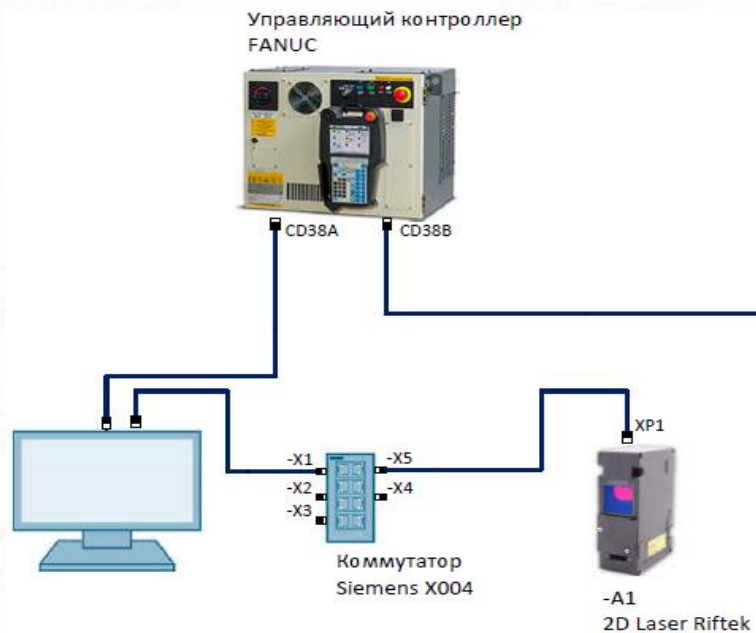
X. Защита технических средств и систем (ЗТС)	ОРД, СКУД, ИБП
XI. Защита информационной (автоматизированной) системы и ее компонентов (ЗИС)	ОРД , СКУД, МЭ, KICS for Nodes / KICS for Networks, KES, TrafficInspector, UserGate, Dallas Lock, SecretNet, UserGate, ФПСУ-IP, Континент, Застава, VipNet, VPN Gate, ФПСУ-IP, Дионис, МР ISIM
XII. Реагирование на компьютерные инциденты (ИНЦ)	VipNet IDS/IPS, COA «Континент», АПК «Рубикон», АМЭ ALTELL NEO, COB Dallas Lock, KSC, MaxPatrol SIEM, R-Vision IRP
XIII. Управление конфигурацией (УКФ)	ОРД, KICS for Nodes / KICS for Networks, KES, KSC
XIV. Управление обновлениями программного обеспечения (ОПО)	ОРД , Dallas Lock, SecretNet, KSC
XV. Планирование мероприятий по обеспечению безопасности (ПЛН)	ОРД
XVI. Обеспечение действий в нештатных (непредвиденных) ситуациях (ДНС)	ОРД, резервное копирование, кластеризация
XVII. Информирование и обучение персонала (ИПО)	ОРД



Виды объектов которые приходилось защищать



Информационные
системы



АСУ ТП



Информационно-
телекоммуникационные
сети



Информационные системы



1. Программное обеспечение
2. Оконечные АРМ
3. Серверы

Система анализа защищенности
Система обнаружения вторжений
Система защиты от НСД
Система антивирусной защиты



Информационно-телекоммуникационная сеть



1. Сетевое оборудование
2. Трафик
3. Общая целостность и неизменность компонентов

IDS/IPS

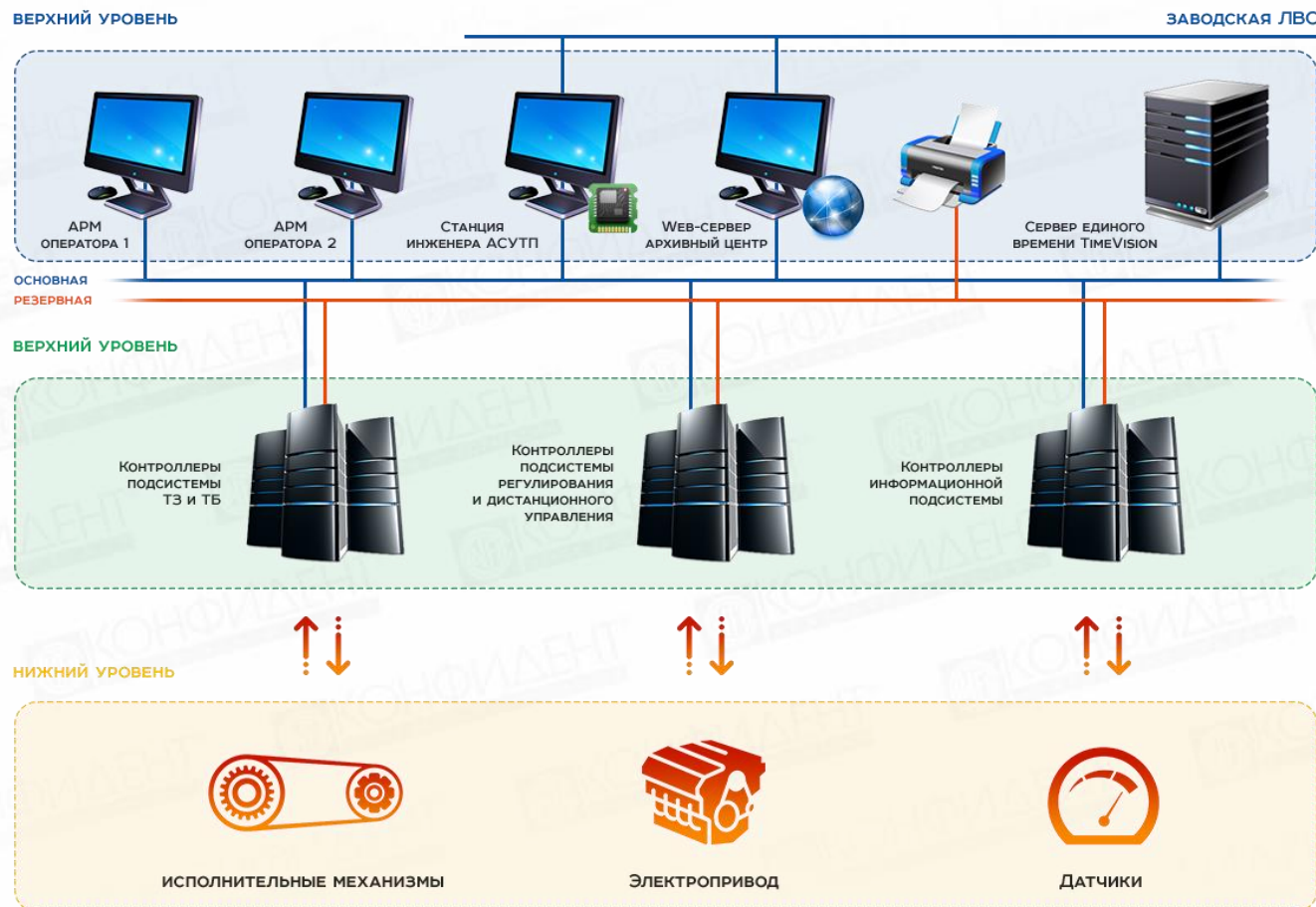
Антивирусная защита

Анализ трафика

МЭ

Сегментирование сети

Обеспечение защиты от НСД

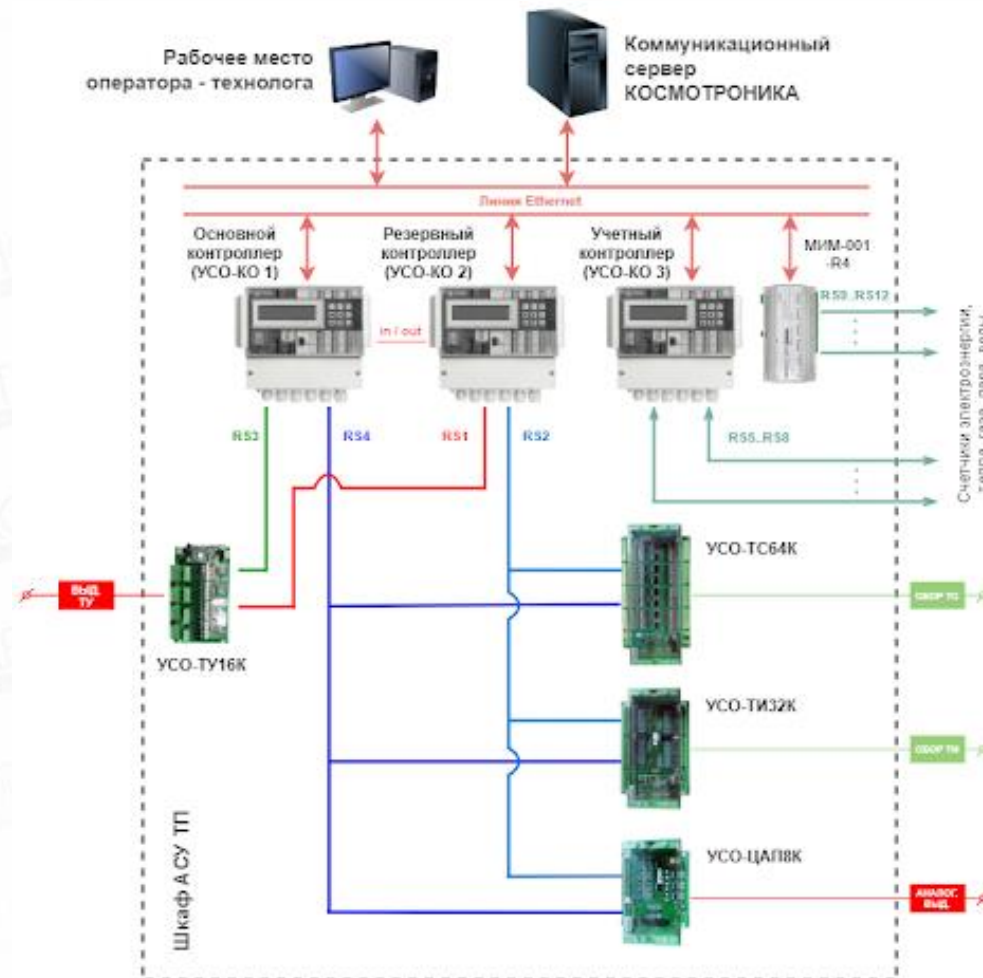


1. Трафик
2. Прошивка ПЛК
3. АРМ инженеров
4. Различное оконечное оборудование
5. Теги, передаваемые с датчиков

Анализ трафика
Антивирусная защита
Сегментирование ТЛВС



Компенсирющие меры





Основные проблемы

1. Неверное определение категории
2. Субъективная трактовка требований законодательства
3. непонимание выбора средств защиты
4. **Разрозненность подразделений – ИБ, ИТ, АСУ**
5. Устаревшее оборудование
6. Импортозамещение





Неверное определение категории

Были выявлены крайности:

1. Нет вообще ЗОКИИ, либо все ЗОКИИ 1 категории
2. Категорировалось абсолютно, либо явно замалчивали об объекте

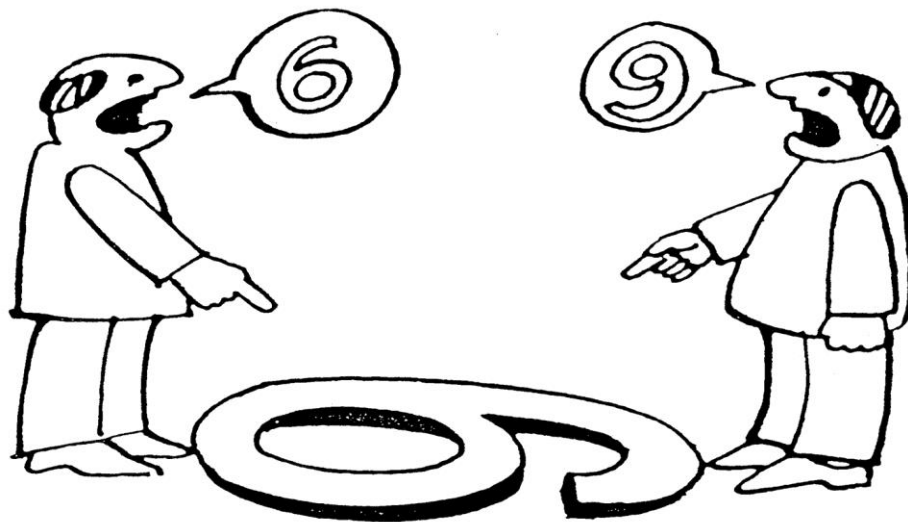




Субъективная трактовка требований

Примеры:

- 1) Аудит безопасности полностью закрывается SIEM-системой
- 2) Установка классического АВЗ на технологические ОИ
- 3) Все требования должны исполняться исключительно СрЗИ





Непонимание выбора средств защиты

Закон начал действовать в 2018 году.

До этого в части предприятий перед ОИБ стояли задачи:

- 1) По защите ПДн
- 2) Организации защиты ГТ
- 3) Закупке и обновлению АВЗ

После начала действия закона ОИБ требовалось очень быстро прокачаться в более сложных или вовсе новых направлениях ИБ





Разрозненность подразделений – ИБ, ИТ, АСУ

Классическая проблема при взаимодействии на большом предприятии подразделений ИБ, ИТ, АСУ





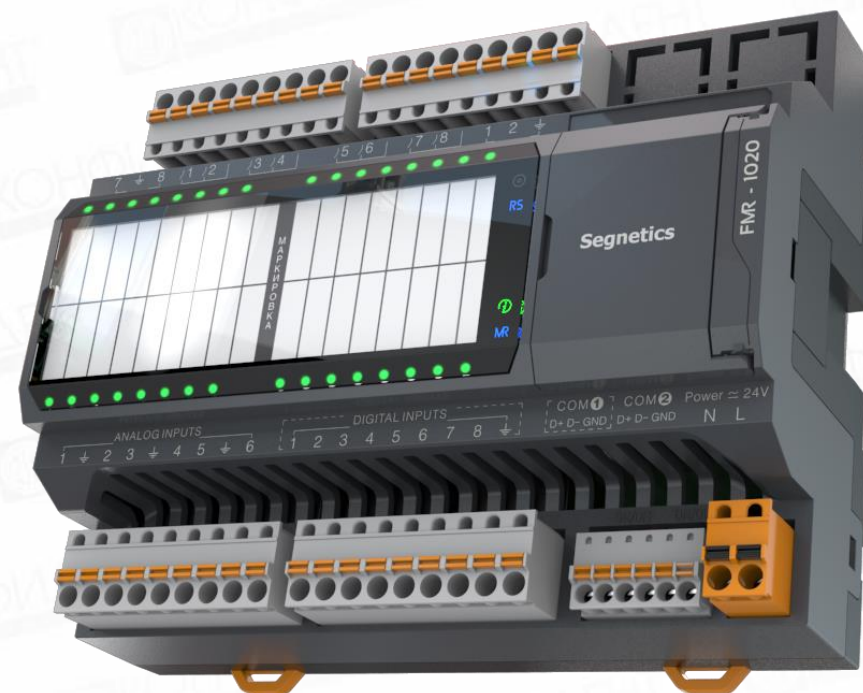
Устаревшее оборудование

Старое технологическое сетевое оборудование не поддерживает Ethernet или SPAN/R-SPAN





Большая проблема при переходе с Siemens, Schneider, Emerson, Segnetics и пр. на отечественные





Задачи которые решаем



1. Категорирование
2. Разработка ОРД (стратегическая безопасность)
3. Подбор СЗИ
4. Проектирование
5. Внедрение
6. Эксплуатация

Советуем через 2 года вернуться к 1 пункту

**«Конфидент-Информация» готова поделиться с Вами
опытом!**



Благодарю за внимание!

Зенков Александр

Руководитель
инженерно-технического
департамента

+7(812) 325-1037, доб. 7985

+7 962-669-50-68

email:zenkov.aleksandr@confident.ru